[illegible]537 - 905630

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE THE APPLICATION OF:	) Examiner: Brandon S. Hoffman
Clive Jones	) Group Art Unit: 2136
Serial No.: 09/913,785	)
	) Customer No. 23644
Filed: January 4, 2001	)
For: Data Encoding/Decoding Device and Apparatus Using the Same	)

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450," on December 23, 2005
Signature Minnie Wilson
Minnie Wilson

BRIEF ON APPEAL

Honorable Director of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

This brief is being filed to support the appeal filed for this application following the Examiner's final Office Action dated May 9, 2005. An appropriate Notice of Appeal was tendered to the Patent and Trademark Office on October 27, 2005 and received on October 31, 2005, and an amendment to reduce the issues for appeal is being filed concurrently herewith to eliminate claims 1-7 and 19-20, in addition to the claims already cancelled.

This brief is being filed with the brief fee pursuant to 37 C.F.R. §41.20(b) (2).

12/29/2005 SHASSEN1 00000015 09913785
01 FC:1402 500.00 OP

(i) Real Party in Interest

This application is assigned to Meridian Audio Ltd., who is the real party in interest. The assignment was recorded on January 14, 2002 at reel 012477, frame 0546.

(ii) Related Appeals and Interferences

There are no known related appeals and interferences.

(iii) Status of Claims

This application was filed with claims 1 through 18, and in a response mailed March 24, 2005, claims 11-18 were cancelled, and claims 19 through 22 were added. By the amendment being filed concurrently herewith, claims 1-7 and 19-20 have further been cancelled. Those claims being appealed are claims 8-10, 21 and 22, and clean versions of the claims are set forth in the Claims Appendix appended hereto.

(iv) Status of Amendments

The only amendment following the final Office Action is the amendment being filed concurrently herewith canceling claims 1-7 and 19-20, and amending claim 8 slightly to correct a typographical error and clarify one term. It is believed that this amendment will be entered without objection.

(v) Summary of Claimed Subject Matter

A problem occurs when transmitting audio data digitally for output. The problem is that sound is output in the analog domain which means that the final drivers driving loudspeakers, headphones etc must inevitably operate in the analog domain, and such drivers are sensitive to picking up the digital signal. A digital signal normally has sharp peaks at certain frequencies, often frequencies related to the clock frequency, and so the digital signal picked up in analog stages can produce a significant degradation in the output quality.

A further factor in the choice of digital signal is the need to be able to recover the clock signal from the transmitted digital signal at the receiving end.

Finally, encoding is often needed when transmitting data, for example to ensure that the digital signals cannot be captured by any device, for example to protect digital audio signals from illegal recording. This gives rise to a further difficulty, in that it is necessary to transmit the encoding key from the transmitter to receiver and this occupies bandwidth in the channel. It is therefore desired to minimize the number of transmitted bits, while still encoding securely.

Thus, what is needed is a way of encoding digital audio data to deal with all these issues.

The invention solves this problem with the apparatus of claim 8. Each bit input into the data encoding device is encoded separately to create an encoded output bit, and the encryption key is updated after encoding each bit of a word.

The design enables the encoded output data to have the properties of white noise so reducing possible interference in analog stages as well as improving the performance of clock recovery in the decoder, while at the same time maintaining the data structure so that standard interface protocols can be used (page 9 lines 23 to 25).

The design also maintains security even if only a limited number of random bits are transmitted from encoder to decoder, for example when transmitting only one new random bit for each word. However, this means that there is a link between the random numbers used to encode subsequent words. In the invention, this relationship is disguised by not simply applying the bits generated by the random number generator, but by using a further unit, the permutation unit, which generates an initial plurality of encoding bits, which as stated in the claim is the encryption key used to generate the initial output bit. Thus, the permutation unit makes it much harder for an eavesdropper to correctly decode the transmitted signal.

(vi) Grounds of Rejection To Be Reviewed On Appeal

There is one ground of rejection being reviewed on appeal, the rejection of claim 8-10, 21 and 22 under 35 U.S.C. §103(a) as being unpatentable over Hustig U.S. Patent No. 4,672,605 in view of Rhoads U.S. Patent No. 5,768,426.

(vii) Argument

Claim 8 stands rejected over Hustig in view of Rhoads. The Examiner contends that Hustig discloses an encoding unit which combines each bit input on the serial data input with a plurality of additional encoding bits forming an encryption key to derive an encoded output bit.

In the preferred embodiments of Hustig, reference numeral (98) is an exclusive OR gate which simply ors a pseudo random code from the pseudo random code generator (102) with bits from the bit interleaver (85). Thus, the unit (98) combines each bit input on the serial data input with a single additional bit, not a plurality of additional encoding bits as specifically recited by claim 8.

Note that in Hustig et al there is no need for such a permutation unit, since the pseudo random code generator is simply switched to the same code (column 10 line 32). This is hardly secure, since if an eavesdropper once determines which code is used, the eavesdropper can listen in using that code without limit. Since in Hustig there are only 255 different codes (column 6 lines 30 to 31), this would be easy simply by trial and error using that code without limit. Since in Hustig there are only 255 different codes (column 6 lines 30 to 31), this would be easy simply by trial and error.

The Examiner contends that Rhoads discloses the additional features not present in Hustig. In particular, the Examiner contends that Rhoads discloses in Figure 7 of Rhoads a permutation unit which generates an initial plurality of encoding bits forming an encryption key from the multiple bit random word. However, even if the table in Figure 7 is identified with the initial plurality of encoding bits, this cannot constitute an encryption key as recited in claim 8. In the claim, the encryption key must comprise the initial plurality of encoding bits, and must be updated at each bit to provide an updated key "which is derived from previous values of the key and of the input bit". Instead, in Hustig, the code words of Figure 7 are constant. Column 22, lines 11-29 clarify that a fixed amount of noise data is stored (lines 27-29) in other words the noise data is kept constant and is not updated bit by bit from previous values of a key and of the input bit.

The Examiner contends that the updated encryption key is disclosed at column 17, line 1 to column 18, line 29 of Rhoads. This passage relates to Figures 5 and 6. It is apparent from Figure 6, and the specification, that Figure 6 does not take a single input bit and a plurality of bits of a key to generate from those bits a single output bit and an updated key.

Instead, the operation of Figure 6 is completely different. Figure 6 shows an input signal (of 8-20 bits - column 17, line 31) being applied to the look-up table (204) which provides an 8-bit digital output word which is combined with an 8-bit digital noise signal from source (206). This is output through second scaler (210) which provides a digital output between -2 and +2. This is essentially a noise signal stored in memory (214). Then, a control word (216) is used to control whether to add or subtract the signal in the memory to the input signal. Since the input signal is an 8-20 bit word, this produces a slightly modified 8-20 bit word.

Thus, Rhoads does not describe taking a single initial bit and an initial key and producing an updated key together with an output bit.

Thus, there is nothing in either Hustig or Rhoads that describes the core of the encoding unit, namely the feature that the initial bit input on the serial data input is encoded with an encryption key comprising the initial plurality of encoding bits output by the permutation unit, and each subsequent input bit is encrypted using an updated key which is derived from previous values of the key and of the input bit.

Thus, a combination of Hustig and Rhoads would not arrive at the present invention as claimed in the appealed claims.

Even if the exclusive OR (98) of Hustig was replaced with the complex arrangement of Rhoads, this would not result in an arrangement where single bits were encoded as recited, but would instead result in an arrangement where multiple bits were input as in Rhoads and output on the telephone line. The bit-wise encoding required by claim 8 would not take place.

The Examiner suggests that it would have been obvious to combine Hustig and Rhoads to provide a digital output word which can be used as a scaling factor, which can be later verified in the case of piracy. However, as explained above, this would not result in the present invention.

It is further noted that a particular benefit of the present invention is that substantially white noise is sent down an audio link. The purpose of the white noise is not, as in Hustig, to render the signal virtually imperceptible to a listener using an audio channel on the same link. Instead, the purpose of the white noise is to avoid interference with audio components which are very sensitive to audio frequency electrical interference. This ensures that a high quality audio output is possible, that jitter on the received clock does not take place, and to ensure a signal that is both encrypted and identifiable.

Thus, neither Hustig nor Rhoads teach how to reduce jitter and/or self-interference on digital audio interfaces, by making a bit stream containing the digital audio signal which is substantially white.

In case the Examiner asserts that the data of Hustig is "whitened", applicants note that this is essentially used to reduce cross-talk (column 6, lines 41-51 of Hustig), not to improve the quality of the received audio signal.

Conclusion

For the reasons set forth above, it is submitted that the Examiner's rejection of claim 8-10, 21 and 22 has been demonstrated to be shown to be clearly in error, and reversal of the Examiner is therefore urged.

December 23, 2005

Respectfully submitted,

William M. Lee, Jr.
Registration No. 26,935
Barnes & Thornburg LLP
P.O. Box 2786
Chicago IL 60690-2786
(312) 214-4800
Fax (312) 759-5646

Claims Appendix

8. An apparatus for generating digital audio data comprising

a source of digital audio signals, and

a data encoding device having:

a serial data input;

an encoded serial data output;

a random number generator which generates a stream of random bits;

a transformation unit comprising means for storing a predetermined number of values of the random bit to derive a multiple bit random word;

a permutation unit which generates an initial plurality of encoding bits from the multiple bit random word; and

an encoding unit which combines each bit input on the serial data input with a plurality of additional encoding bits forming an encryption key, to derive an encoded output bit and an updated encryption key comprising a plurality of updated encodes bits, wherein an initial bit input on the serial data input is encoded with an encryption key comprising the initial plurality of encoding bits output by the permutation unit and each subsequent input bit is encrypted using an updated key which is derived from previous values of the key encryption and of the input bit, and wherein over time the encoded output bit stream comprises substantially white noise.

9. An apparatus as claimed in claim 8, wherein the output at the output port is in SPDIF or AES/EBU format.

10. An apparatus as claimed in claim 8, comprising a compact disc player.

21. An apparatus for reconstructing digital audio signals comprising:

an input for receiving encoded digital audio signals;

a receiver for supplying the encoded digital audio signals to a decoding device;

and an output for the reconstructed digital audio signal; and

a decoding device comprising:

a serial data input;

a transformation unit comprising means for storing a predetermined number of values of random bits to derive a multiple bit random word;

a permutation unit which generates an initial plurality of bits from the multiple bit random word; and

an decoding unit which combines each bit input on the serial data input with a plurality of additional encoding bits forming a key, to derive an decoded output bit and an updated key comprising a plurality of updated bits, wherein an initial bit input on the serial data input is decoded with a key comprising the initial plurality of bits output by the permutation unit and each subsequent input bit is decrypted using an updated key which is derived from previous values of the key and of the input bit.

22. A data communications system comprising:

a data encoding device comprising:

a serial data input;

an encoded serial data output;

a random number generator which generates a stream of random bits;

a transformation unit comprising means for storing a predetermined number of values of the random bit to derive a multiple bit random word;

a permutation unit which generates an initial plurality of encoding bits from the multiple bit random word; and

an encoding unit which combines each bit input on the serial data input with a plurality of additional encoding bits forming an encryption key, to derive an encoded output bit and an updated encryption key comprising a plurality of updated encodes bits, wherein an initial bit input on the serial data input is encoded with an encryption key comprising the initial plurality of encoding bits output by the permutation unit and each subsequent input bit is encrypted using an updated key which is derived from previous values of the key and of the input bit, and wherein over time the encoded output bit stream comprises substantially white noise; and

a decoding device comprising:

a serial data input;

Evidence Appendix and Related Proceedings Appendix

There is no Evidence Appendix or Related Proceedings Appendix.